Indian J. Phys. **80** (5), 495-499 (2006)

IJP

A mathematical criterion for single photon sources used in quantum cryptography

Anirban Pathak

Department of Physics, Jaypee Institute of Information Technology, A-10, Sector-62, Noida-201 307, Uttar Pradesh, India

E-mail : anirbanpathak@yahoo.co.in

Abstract : A single photon source (SPS) is very important for quantum computation. In particular, it is essential for secured quantum cryptography. But there is no perfect SPS in reality. Therefore, probabilistic SPS where probability of simultaneous emission of two, three, four and more photon is less than the emission of a single photon are used. Since classical photon always comes in bunch, the required single photon source must be nonclassical. In the well-known antibunched state, the rate of simultaneous emission of two photon is less than that of single photon. But the requirement of quantum cryptography is a multiphoton version of the antibunched state or the higher order antibunched state. Recently we have reported a mathematical criterion for higher order antibunching. Here we have shown that any proposal for SPS to be used in quantum cryptography should satisfy this criterion. We have studied four wave mixing as a possible candidate of single photon source.

Keywords : Quantum cryptography, higher order antibunching, third-order nonlinear media

PACS Nos. : 03.67.Dd, 42.65.-k, 42.50.-p

1. Introduction

At present, we normally use RSA cryptographic technique [1] for secured com-munication. The trick behind the success of this most popular public key crypto system lies in the fact that a classical computer takes huge time to factorise a large number, whose factors are two large prime numbers. But this trick will not be valid if we can construct a scalable quantum computer. This is because a quantum computer can use Shor's algorithm [2] to factorise a large number in a polynomial time. This observation have intensified the interest on infinitely secured cryptographic techniques and Bennett and Brassard's 1984 proposal [3] for a infinitely secured protocol for quantum cryptography (BB84 protocol) have received the attention of the whole community. This protocol does not require any quantum computer, so the problem with scalability or decoherence is not important in this context and thus it is expected that the quantum cryptographic technique will appear in the market much before the appearance of a quantum computer. Recent experimental observations [4,5], do indicates this fact. For example, we can note the recent success in free space distribution of entangled photon pairs over a noisy ground atmosphere of 13 km [4].

The basic problem with BB84 protocol is that it needs a source that can generate single photon on demand. This is because if it produces some pulses with multiple photons (say N photons) and Eve take one of them and allow rest of the photon (N-1 photons) to reach Bob, then even after the comparison with Alice's bits Bob will not be able to detect the existence of Eve. So the system is no more infinitely secured. To get the advantage of infinite security we need perfect single photon source. But in reality there does not exist any perfect single photon source (by perfect we mean a source which never produces two or more photon simultaneously). The single photon sources, that are available are probabilistic in nature. A probabilistic single photon source produces single photon in most of the time but there is a finite probability of producing multiphoton pulse. The less is this probability the better is the source. Keeping this in mind we can say that in a probabilistic single photon source the probability of emission of single photon should be greater than a two photon pulse and that must be greater than a three photon pulse and so on. Classically photon always comes in group, and they are called bunched. When the opposite situation occurs, and the probability of simultaneous detection of two photon become less than the probability of their detection after a time interval t then they are called anibunched. This is a completely nonclassical state [6,7] (it does not have any classical analogue). For implementation of BB84 protocol we need a multiphoton version of antibunching (*i.e.* a higher order version of well known antibunching phenomenon) and that is called higher order antibunching.

Higher order extension of the nonclassical effects have been introduced in recent past [8–11]. Among these higher order nonclassical effects higher order squeezing is studied in detail [8,9,12,13] but the higher order antibunching which is required for implementation of BB84 protocol is not yet studied rigorously. Actually, Lee introduced an inequality as the criteria for higher order nonclassical state in a pioneering paper [10] by using the negativity of the P function [6]. A nonclassical state satisfying Lee's criteria is called higher order antibunched state and is theoretically predicted to be observable in two photon coherent state [10] and trio coherent state [14]. But from the earlier works of Lee and others [10,11,14] physical meaning of the criteria is not clear. Recently, Pathak and Garcia [15] have given a simplified condition for higher order antibunching. In the next section, we have briefly described BB84 protocol. In Section 3, we have derived a simple condition that a SPS, which will be used in quantum cryptography, has to satisfy. In Section 4, we have shown that the condition is satisfied by pump mode of a four wave mixing process. The last section is dedicated for concluding remarks.

2. BB84 protocol

The protocol is very simple, Alice wants to send a message to Bob in secured manner and they have chosen photon polarized along a particular polarization axis (say horizontal) as '0' and photons polarized along the axis perpendicular to it as '1'. Now if she sends a horizontally polarized photon that will mean 0 and if she sends a vertically polarized photon that will mean 1. The choice of horizontal and vertical axes are not unique, in fact there are infinitely many possibilities. If somebody named Eve wants to crack the information he has to measure this photon in a particular basis (one out of infinity, so the probability of axis matching is almost zero) and if that basis does not coincide with the basis of Alice and Bob, then there will be a finite probability of getting the bit incorrect (correct). After the measurement, Eve has to reproduce the bit according to his axis, since cloning is not allowed. This will not match with Bob's axis. So there will be a finite probability that Bob's measurement yield a wrong result. Now, by comparing some bits with Alice, the existence of Eve can be traced by Bob. Thus, it is infinitely secured against the attack of Eve, provided you have a single photon source.

3. Mathematical condition for single photon source

The i-th factorial moment of usual number operator is defined as, $N^{(i)} = N(N-1)........(N-i+1)$. At first we will try to understand the meaning of $\left\langle N^{(i)}\right\rangle$, where $\langle\ \rangle$ denotes the quantum average. From the operator ordering theorems it is easy to show that

$$a^{\dagger i}a^{i} = N^{(i)} \tag{1}$$

and thus basically we need the physical meaning of $\left\langle a^{\dagger i}a^{i}\right\rangle$ which can be understood with the help of n-th order correlation function G^{n}.

The n-th order correlation function for an electromagnetic field is in general defined as

$$\begin{aligned} & G^{(n)}(x_1 \dots x_n, y_m \dots y_1) \\ & = \left\langle E^{-}(x_1)\dots E^{-}(x_n)\dots E^{+}(y_n)\dots E^{+}(y_1)\right\rangle, \end{aligned} \tag{2}$$

where $x_j = (r_j, t_j)$ and $y_j = (r_{j+m}, t_{j+m})$. In case of a quantum field the average in the right hand side of (2) is a quantum average. Otherwise the above definition of n-th order correlation is valid in general and in quantum optics it is used to study the higher order coherence [6]. Now if we look at a single point then n-th order correlation function (2) reduces to

$$\begin{aligned} G^{(n)}(x_1 \dots x_1) & = \left\langle E^{-}(x_1)\dots E^{-}(x_1)E^{+}(x_1)\dots E^{+}(x_1)\right\rangle \\ & = \left\langle E^{-}(x_1)E^{+n}(x_1)\right\rangle. \end{aligned} \tag{3}$$

Here, the single point means that the correlation or the coherence is observed at a particular point in space at a particular time. This definition of single point n-th order correlation function or coherence function can alternatively be written in a normalized form as

$$G^{(n)}(x_1 \dots x_1) = \left\langle a^\dagger a^\dagger \dots a^\dagger a \dots aa \right\rangle = \left\langle a^{\dagger n} a^n \right\rangle. \qquad (4)$$

This single point correlation function is a measure of correlation between n photons of the same mode. Therefore, $\left\langle a^{\dagger n} a^n \right\rangle$ is a measure of the probability of observing n photons of the same mode at a particular point in space time coordinate.

After realising the physical meaning of $\left\langle N^{(i)} \right\rangle$, we would like to extend it into new inequalities and extract some physical information out of them. Let us start from our physical requirement that a single photon source to be used in quantum cryptography has to satisfy : The probability of emission of single photon should be greater than a two photon pulse and that must be greater than a three photon pulse and so on. This condition can now be written as

$$\left\langle N_x^{(l+1)} \right\rangle < \left\langle N_x^{(l)} \right\rangle \langle N_x \rangle < \left\langle N_x^{(l-1)} \right\rangle.$$

$$\times \langle N_x \rangle \langle N_x \rangle < \dots < \langle N_x \rangle^{l+1} \qquad (5)$$

Therefore, under the antibunching condition if we observe $(l + 1)$ photons then the probability of getting them 'one by one' is maximum and the probability of getting all the $(l + 1)$ photons at a bunch is minimum. This is what the idea of antibunching is. If we just reverse the direction of inequality and look for bunching of photons then for l-th order bunching the possibility of getting all $(l + 1)$ photons in a bunch will be maximum.

The idea of antibunching was introduced just in opposite to bunching and essentially that idea is manifested here. If we observe total $(l + m)$ number of photons, it is possible to get them in different combinations, for example we can get all the photons in a bunch or l at a bunch and m in another bunch and like wise. In the nonclassical region of antibunching, the probability of getting all the photons separately (one by one) is always maximum.

With the help of (5), we can simplify the condition for obtaining l-th order antibunching as

$$d(l) = \left\langle N_x^{(l+1)} \right\rangle - \langle N_x \rangle^{l+1} < 0. \qquad (6)$$

Here, we can note that $d = 0$ and $d > 0$ corresponds to higher order coherence and higher order bunching (many photon bunching) respectively. This is the condition that has to be satisfied by any candidate of SPS.

4. The search for single photon source

At present, we cannot produce single photon source (SPS) in true sense. All the available SPS are probabilistic in nature. In any candidate for probabilistic SPS, the probability of getting isolated photon must be maximum and probability of getting a pulse of two or more photon should decrease with the increase of photon number. Thus, it has to satisfy the criterion for higher order antibunching derived in last section. Our task is to check whether well-known optical processes can satisfy the criteria or not. Since these states are essentially nonclassical, we have chosen a physical system which are already known to produce nonclassical effect. The optical process which we will study here as a possible candidate is four wave mixing process.

4.1. Four wave mixing process :

Four wave mixing may happen in different ways. One way is that two photon of frequency ω_1 are absorbed (as pump photon) and one photon of frequency ω_2 and another of frequency ω_3 are emitted. The Hamiltonian representing this particular four wave mixing process is

$$H = a^\dagger a\omega_1 + b^\dagger b\omega_2 + c^\dagger c\omega_3 + g(a^{\dagger 2} bc + a^2 b^\dagger c^\dagger), \qquad (7)$$

where a and $a^\dagger$ are annihilation and creation operators in pump mode which satisfy $\left[a, a^\dagger\right] = 1$; similarly, b, $b^\dagger$ and c, $c^\dagger$ are annihilation and creation operators in stokes mode and signal mode, respectively and g is the coupling constant. Substituting $A = ae^{i\omega_1 t}$, $B = be^{i\omega_2 t}$ and $C = ce^{i\omega_3 t}$, we can write the Hamiltonian (7) as

$$H = A^\dagger A\omega_1 + B^\dagger B\omega_2 + C^\dagger C\omega_3 + g(A^{\dagger 2} BC + A^2 B^\dagger C^\dagger). \qquad (8)$$

Since we know the Hamiltonian, we can use Heisenberg's equation of motion (with $\hbar = 1$)

$$\dot{A} = \frac{\partial A}{\partial t} + i[H, A] \qquad (9)$$

and short time approximation to find out the time evolution of the essential operators. From eq. (8) we have

$$[H, A] = -A\omega_1 - 2gA^\dagger BC. \qquad (10)$$

From (9) and (10), we have

$$\dot{A} = iA\omega_1 - iA\omega_1 - i2gA^\dagger BC = -2igA^\dagger BC. \qquad (11)$$

Similarly,

$$\dot{A} = -2igA^2 C^\dagger \qquad (12)$$

and

$$\dot{C} = -gA^2B^\dagger . \tag{13}$$

We can find the second order differential of A using eqs. (9 and 11–13) as

$$\ddot{A} = \frac{\partial \ddot{A}}{\partial t} + i[H, \dot{A}] = 4g^2AB^\dagger BC^\dagger C$$

$$-2g^2A^\dagger A^2B^\dagger B - 2g^2A^\dagger A^2C^\dagger C - 2g^2A^\dagger A^2. \tag{14}$$

Now by substituting (11) and (14) in the Taylor's series expansion

$$f(t) = f(0) + t\left(\frac{\partial f(t)}{\partial t}\right)_{t=0}$$

$$\frac{\partial^2 f(t)}{2!\left(\partial t^2\right.}\Big)_{t=0} \tag{15}$$

we obtain

$$A(t) = A - 2igtA^\dagger BC + \frac{g^2t^2}{2!}$$

$$\left[4AB^\dagger BC^\dagger C - 2A^\dagger A^2B^\dagger B - 2A^\dagger A^2C^\dagger C - 2A^\dagger A^2\right]. \tag{16}$$

The Taylor series is valid when t is small, so this solution is valid for a short time and that is why it is called short time approximation. The above calculation is show as an example. Similarly, we can find out time evolution of B and C or any other creation and annihilation operator that appears in the Hamiltonian of matter field interaction. This is a very strong technique since this straight forward prescription is valid for any optical process where interaction time is short. Now we can use this solution to check whether it satisfies the condition (6) or not.

Let us start with the study of the possibility of observing first order anti-bunching. From eq. (16), we can derive expression for $N(t)$ and $N^{(2)}(t)$ as

$$N(t) = A^\dagger A + 2igt(A^2B^\dagger C^\dagger - A^{\dagger 2}BC)$$

$$+g^2t^2(8A^\dagger AB^\dagger BC^\dagger C - 4B^\dagger BC^\dagger C)$$

$$-g^2t^2(2A^{\dagger 2}A^2B^\dagger B + 2A^{\dagger 2}A^2C^\dagger C + 2A^{\dagger 2}A^2) \tag{17}$$

and

$$N^{(2)}(t) = A^{\dagger 2}A^2 - 4igtA^{\dagger 3}ABC + 4igtA^{\dagger 2}BC$$

$$4igtA^\dagger A^3B^\dagger C^\dagger + 2igtA^2B^\dagger C^\dagger$$

$$+g^2t^2(24A^{\dagger 2}A^2B^\dagger BC^\dagger C +$$

$$32A^\dagger AB^\dagger BC^\dagger C + 4B^\dagger BC^\dagger C)$$

$$-g^2t^2(4A^{\dagger 4}B^2C^2 + 4A^4B^{\dagger 2}C^{\dagger 2} + 4A^{\dagger 3}A^3B^\dagger B$$

$$+4A^{\dagger 3}A^3C^\dagger C + 2A^{\dagger 2}A^2B^\dagger B + 2A^{\dagger 2}A^2C^\dagger C)$$

$$-g^2t^2(4A^{\dagger 3}A^3 + 2A^{\dagger 2}A^2). \tag{18}$$

In the present study, all the expectations are taken with respect to $|\alpha > |0 > |0 >$ for simplification. This assumption physically means that initially a coherent state (say, a laser) is used as pump and before the interaction of the pump with atom, there was no photon in b or c mode. Thus, the pump interacts with atom and causes excitation followed by emission. Now from eqs. (17) and (18) we have

$$\langle N\rangle^2 = |\alpha|^4 - 4g^2t^2|\alpha|^6, \tag{19}$$

$$\left\langle N^{(2)}(t)\right\rangle^2 = |\alpha|^4 - g^2t^2\left(-4|\alpha|^6 - 2|\alpha|^4\right) \tag{20}$$

where $A|\alpha> = \alpha|\alpha>$.

Now using eqs. (19) and (20), we can show that the four wave mixing process satisfies the criterion of antibunching (6) because :

$$d(1) = \left\langle N^{(2)}(t)\right\rangle - \langle N\rangle^2$$

$$= \left[|\alpha|^4 + g^2t^2\left(-4|\alpha|^6 - 2|\alpha|^4\right)\right]$$

$$-\left[|\alpha|^4 - 4g^2t^2|\alpha|^6\right] \tag{21}$$

is always negative. Essentially, this is a nonclassical state but mere satisfaction of nonclassicality or antbunching is not enough we need a source which can satisfy the condition for higher order antibunching. So, let us see what happens in the next higher order that is in the second order.

For the study of calculation of second order of antibunching, we can calculate $A^3(t)$ simply by multiplication and operator ordering :

$$A^3(t) = A^3 - 6igtA^\dagger A^2BC - 6igtABC$$

$$+g^2t^2(6A^3B^\dagger BC^\dagger C)$$

$$-g^2t^2(3A^\dagger A^4B^\dagger B + 3A^3B^\dagger B$$

$$+3A^{\dagger}A^4C^{\dagger}C+3A^3C^{\dagger}C)$$
$$-g^2t^2(3A^{\dagger}A^4+3A^3+12A^{\dagger 2}AB^2C^2$$
$$+12A^{\dagger}B^2C^2)\,. \qquad (22)$$

Then $A^{\dagger^3}(t)$ can be written simply as,

$$A^{\dagger^3}(t)=A^{\dagger^3}+6igtA^{\dagger 2}AB^{\dagger}C^{\dagger}+6igtA^{\dagger}B^{\dagger}C^{\dagger}$$
$$+g^2t^2(6A^{\dagger 3}B^{\dagger}BC^{\dagger}C)$$
$$-g^2t^2(3A^{\dagger 4}AB^{\dagger}B+3A^{\dagger 3}B^{\dagger}B$$
$$+3A^{\dagger 4}AC^{\dagger}C+3A^{\dagger 3}C^{\dagger}C)$$
$$-g^2t^2(3A^{\dagger 4}+3A^{\dagger 3}$$
$$12A^{\dagger}A^2B^{\dagger 2}C^{\dagger 2}+12AB^{\dagger 2}C^{\dagger 2}). \qquad (23)$$

Last two equations can be used to calculate the third factorial moment ($N^{(3)}(t)$) of number operator N as

$$N^{(3)}(t)=A^{\dagger 3}A^3-6igtA^{\dagger 4}A^2BC-6igtA^{\dagger 3}ABC$$
$$-6igtA^{\dagger 2}A^4B^{\dagger}C^{\dagger}-6igtA^{\dagger}A^3B^{\dagger}C^{\dagger}$$
$$+g^2t^2(48A^{\dagger 3}A^3B^{\dagger}BC^{\dagger}C+108A^{\dagger 2}A^2B^{\dagger}BC^{\dagger}C$$
$$+36A^{\dagger}AB^{\dagger}BC^{\dagger}C)$$
$$-g^2t^2(6A^{4\dagger}A^4B^{\dagger}B+6A^{\dagger 3}A^3B^{\dagger}B$$
$$+6A^{\dagger 4}A^4C^{\dagger}C+6A^{\dagger 3}A^3C^{\dagger}C+6A^{\dagger 4}A^4)$$
$$-g^2t^2(6A^{\dagger 3}A^3+12A^{\dagger 5}AB^2C^2$$
$$+12A^{\dagger 4}B^2C^2+12A^{\dagger}A^5B^{\dagger 2}C^{\dagger 2}+12A^4A^5B^{\dagger 2}C^{\dagger 2})\,. \qquad (24)$$

Taking expectation value with respect to the intial state we can write

$$\left\langle N^{(3)}(t)\right\rangle=A^{\dagger 3}A^3+g^2t^2(-6A^{\dagger 4}A^4-6A^{\dagger 3}A^3)$$
$$=|\alpha|^6-g^2t^2\left(6|\alpha|^8+6|\alpha|^6\right).$$

On the other hand, we can calculate $\langle N\rangle^3$ as

$$\langle N(t)\rangle^3=|\alpha|^6-6g^2t^2|\alpha|^8\,. \qquad (25)$$

By using last two equations, one can easily check that pump mode photon of four wave mixing process satisfy the criteria of antibunching of second order (6). Since,

$$d(2)=\left[|\alpha|^6-g^2t^2\left(6|\alpha|^8+6|\alpha|^6\right)\right]$$
$$-\left[|\alpha|^6-6g^2t^2|\alpha|^8\right]$$
$$=-6g^2t^2|\alpha|' \qquad (26)$$

5. Conclusion

From (21) and (26), we can observe that the degree of nonclassicality increases monotonically with $|\alpha|^2$ (the avearge photon number before the interaction). This monotonic increase in nonclassicality is expected to cease with the introduction of higher order terms. But comparing (21) and (26), we can easily conclude that for the same values of g, t and $|\alpha|$, second order antibunching is more nonclassical than the usual first order antibunching. In other words, we can say, since $d(2)$ is more negative than $d(1)$, so the depth of nonclassicality is more in second order antibunching. This coincides exactly with the expected property of higher order antibunching discussed in Ref. [15]. Finally, we would like to conclude that the four wave mixing process may be a possible source of single photon needed for quantum cryptography.

Acknowledgments

Author thanks his student Mr. Prakash Gupta for his efforts to reproduce and crosscheck some of the equations and for his interesting questions and comments. He is also thankful to the DST, India for partial financial support.

References

[1] R Rivest, A Shamir and L Adleman *MIT Laboratory for Computer Science, Technical report, MIT/LCS/TR-212* (1979)

[2] P Shor *S I A M J Computing* **26** 1484 (1997)

[3] C H Bennett and G Brassard *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, IEEE*, (New York) (1984)

[4] C Z Peng *et al, Phys. Rev. Lett.* **94** 150501 (2005)

[5] L P Lamoureux *et al, Phy. Rev. Lett.* **94** 050503 (2005)

[6] P Meystre and M Sargent *III Elements of Quantum Optics* (Berlin : Springer-Verlag) (2nd ed) p1 (1991)

[7] V V Dodonov *J. Opt. B : Quant. Semiclass. Opt.* **4** R1 (2002)

[8] C K Hong and L Mandel *Phys. Rev. Lett.* **54** 323 (1985)

[9] C K Hong and L Mandel *Phys. Rev.* **A32** 974 (1985)

[10] C T Lee *Phys. Rev.* **A41** 1721 (1990)

[11] C T Lee *Phys. Rev.* **A41** 1569 (1990)

[12] M Hillery *Phys. Rev.* **A36** 3796 (1987)

[13] D K Giri and P S Gupta *Opt. Commun.* **221** 135 (2003)

[14] N B An *J. Opt. B : Quant. Semiclass. Opt.* **4** 222 (2002)

[15] A Pathak and M Garcia (communicated).